IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

SECURITYPROFILING, LLC, Plaintiff/Counterclaim-Defendant, v. TREND MICRO AMERICA, INC. and TREND MICRO INCORPORATED, Defendants/Counterclaim-Plaintiffs.	§ § § § § § § § § § §	Civil Action No. 3:17-CV-1484-N

DEFENDANTS' RESPONSIVE CLAIM CONSTRUCTION BRIEF

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

Cases

TABLE OF AUTHORITIES
(continued)

Page(s)

Statutes

I. INTRODUCTION

SecurityProfiling's brief advances a variety of often contradictory arguments in support of one apparent goal: to stretch the claims to capture technology, such as security applications that are agnostic to vulnerabilities, which it never purported to invent and that the patents themselves do not purport to cover. These arguments fall into two categories and none warrants adopting SecurityProfiling's constructions in view of the law and the patents' disclosures.

First, SecurityProfiling seeks constructions that would broaden terms (some boundlessly) in a manner that is contrary to their established meanings, the clear disclosure of the patents-in-suit, and often the language of the claims themselves. Such constructions are improper under controlling law but would also permit a fundamental departure from what was purportedly invented and patented.

Second, by arguing against the application of § 112, ¶ 6 to software "code" limitations that are claimed in purely functional terms, SecurityProfiling seeks to sidestep the disclosure and claim construction requirements of the Patent Act and obtain claim scope wholly untethered from the patents' description of a rather narrow invention. In doing so, SecurityProfiling relies almost entirely upon cases decided before the Federal Circuit's seminal *en banc* decision in *Williamson* to advance arguments rejected by a number of courts since *Williamson*. None of SecurityProfiling's arguments changes—nor really challenges—the fact that its patents claim generic software "code" in purely functional terms without providing corresponding algorithms for how to achieve such functions. The Federal Circuit has repeatedly made clear that this is insufficient and that such claims are indefinite as a matter of law.

II. RELEVANT LEGAL STANDARDS

Contrary to many of the positions taken in SecurityProfiling's claim construction brief, "[t]he only meaning that matters in claim construction is the meaning in the context of the

patent" because the claims "are part of a fully integrated written instrument, consisting principally of a specification that concludes with the claims." *Trustees of Columbia Univ. v. Symantec Corp.,* 811 F.3d 1359, 1363-64 (Fed. Cir. 2016). The Federal Circuit has "recognized that when a patent 'repeatedly and consistently' characterizes a claim term in a particular way, it is proper to construe the claim term in accordance with that characterization." *See GPNE Corp. v. Apple Inc*., 830 F.3d 1365, 1370 (Fed. Cir. 2016). Accordingly, it is not only proper, but necessary under Federal Circuit jurisprudence to construe claim terms in accordance with the specification and purported invention. *See, e.g.*, *Wi-LAN USA, Inc. v. Apple Inc.*, 830 F.3d 1374, 1382 (Fed. Cir. 2016) ("specification's consistent references to multiple 'specified connections' . . . weigh[s] in favor of a construction excluding embodiments where the intermediary node is capable of maintaining only one 'specified connection.'").

A claim term "can operate as a substitute for 'means' in the context of § 112, para. 6" where it provides only "a generic description for software or hardware that performs a specified function." *Williamson v. Citrix Online, LLC*, 792 F.3d 1339, 1349-50 (Fed. Cir. 2015).. A term claimed in means-plus-function form must satisfy the definiteness requirements of § 112, ¶ 2, which require that the specification "particularly point out and distinctly claim" the subject matter of the invention. *Blackboard, Inc. v. Desire2Learn, Inc.*, 574 F.3d 1371, 1382 (Fed. Cir. 2009). Where, as here, a challenger argues that terms that do not expressly state "means" should be governed by § 112, ¶ 6, the challenger's "burden must be met by a preponderance of the evidence." *Apex Inc. v. Raritan Computer, Inc.*, 325 F.3d 1364, 1372 (Fed. Cir. 2003).

III. DISPUTED CLAIM CONSTRUCTIONS

A. "vulnerability" (Claim Term 1 – see Ex. 1-A at A8)

While SecurityProfiling's brief suggests that "vulnerability" is a "common term" that need not be burdened with a proper construction, Dkt. 94 at 8, it nonetheless concedes it is a term

that requires construction. Trend Micro's opening brief detailed how its proposed construction—"a device configuration (including installed software) that can be exploited by an attack against [a/the] device"—is required by the language of the claims, confirmed by the specification (which repeatedly and consistently refers to "vulnerabilities" in this manner), and supported by the proffered extrinsic evidence. *See* Dkt. 91 at 4-8. In response, SecurityProfiling largely avoids the inventors' description and use of the term "vulnerability," citing as many different dictionary definitions as passages from the specifications at issue. SecurityProfiling offers no argument warranting a different construction for four main reasons.

First, SecurityProfiling's construction relies upon the vague phrase "security weakness," which deprives the term of any meaningful bounds and will provide little guidance to a jury. The patents never use the phrase "security weakness" in describing a vulnerability and it appears SecurityProfiling seeks to introduce the phrase in the hopes of arguing it encompasses security applications, such as anti-virus scanners, that do not take into account vulnerability information. Indeed, SecurityProfiling's own arguments reveal how far it believes it can stretch the term. For example, SecurityProfiling contends that its view of the claimed "vulnerability" does not even have to exist on a computing device but rather broadly extends to "personnel" or the "physical layout" of networks.[1] *See* Dkt. 94 at 9-10. SecurityProfiling does not and cannot explain how such "security weakness[es]" could possibly be detected and remediated by a software application as required by the claims and emphasized throughout the specification.

[1] Trend Micro did not purport to rely on the glossary found on its website that is not otherwise contemporaneous in time with the patents. *See* Dkt. 94 at 10. Trend Micro did not proffer the glossary and merely noted that SecurityProfiling's own purported extrinsic evidence did not support the breadth of the construction it seeks. *See* Dkt. 91 at 7. Regardless, notwithstanding SecurityProfiling's reliance on the word "typically" to attempt to excise half of the definition it proffered, the glossary indisputably links vulnerabilities to "programs and operating systems," which is reflected nowhere in SecurityProfiling's construction. *See* Dkt. 92, Ex. 1-C at A135.

Second, SecurityProfiling has no meaningful response to Trend Micro's detailing how the claims make clear that attacks are directed to vulnerabilities on devices. *See, e.g.*, Dkt. 91 at 5 (quoting '644 Patent, Claim 1: "determining that the plurality of devices is actually vulnerable to at least one actual vulnerability based on the identified at least one configuration"). Instead, SecurityProfiling mischaracterizes Trend Micro's construction as "vulnerabilities that attack 'devices.'" *See* Dkt. 94 at 8. This is not Trend Micro's construction and it makes no sense. Vulnerabilities do not attack anything. Rather "attacks" are directed to and seek to take advantage of vulnerabilities on devices, as reflected in the claim language, the specification, the extrinsic evidence, and Trend Micro's construction. *See* Dkt. 91 at 4-8.

Third, tacitly acknowledging that the claim language confirms Trend Micro's construction is correct, SecurityProfiling brief effectively rewrites the claim through a cropped and altered quotation. SecurityProfiling purports to quote claim 1 of the '644 Patent as stating that an "'actual vulnerability [is] based on the identified at least one configuration.'" Dkt. 94 at 8-9. It then points to this language and argues against construing a vulnerability in terms of a "device configuration" because its quoted language shows that a vulnerability is only "based on" on a device configuration. *See id.* However, the actual language of the claim element makes clear that it is a "determin[ation]" that is "based on" a device configuration. The full language with SecurityProfiling's proffered quotation emphasized, provides:

> "determining that the plurality of devices is actually vulnerable to at least one ***actual vulnerability [is] based on the identified at least one configuration***"

In view of the claim language as written, SecurityProfiling's argument that Trend Micro's construction renders the claim "internally inconsistent" falls apart. *See id.* Moreover, even under SecurityProfiling's articulation, a vulnerability is plainly tied to a device's configuration (not some amorphous "security weakness"). This is fully consistent with and supportive of

Trend Micro's construction, which is not merely "a device configuration" without more, but rather "a device configuration (including installed software) that can be exploited by an attack against [a/the] device." This introduces no inconsistency within the claims. As discussed above and in its opening brief, Trend Micro's construction is fully supported by the claim language.

Fourth, the bulk of SecurityProfiling's argument—including both of its two citations to the specification—is devoted to attacking a straw-man construction rather than the one actually proposed by Trend Micro. SecurityProfiling equates Trend Micro's construction to just "device configuration" without more and then attempts to contrast this against the specification. *See* Dkt. 94 at 9. Again, as noted above, Trend Micro's construction is not so limited and its actual language dispels SecurityProfiling's manufactured inconsistencies. For example, SecurityProfiling emphasizes the specifications reference to "software patch, policy, and configuration status," each of which is consistent with Trend Micro's construction, which provides "a device configuration (including installed software) . . . ." *Compare id.* at 9 *with id.* at 7 (listing Trend Micro's construction). Indeed, Trend Micro cited virtually identical language from the specification in support of its proposed construction. *See* Dkt. 91 at 6 and n.4. Similarly, the specification's statement "to protect against a known vulnerability," also emphasized by SecurityProfiling, makes perfect sense in view of Trend Micro's actual construction. *See* Dkt. 94 at 7, 9. SecurityProfiling offers no argument as to why it would not be sensible to protect against a known device configuration "***that can be exploited by an attack against [a/the] device***"—nor could it, as this is repeatedly described as the core of its purported invention (not merely dealing with some abstract "security weakness"). *See id.*

B. <u>"intrusion prevention system" (Claim Term 2 – see Ex. 1-A at A8)</u>

SecurityProfiling largely agrees with Trend Micro's construction, which is consistent with the claim language, the specification and the proffered extrinsic evidence. SecurityProfiling

disputes whether the intrusion prevention system monitors "packets" of network traffic and takes action in "real time." Initially, in the joint claim construction statement, SecurityProfiling pointed to an assortment of extrinsic evidence definitions in support of its construction. *See* Dkt 88-1, Ex. A at 2. However, after Trend Micro pointed out how such evidence supported its construction as to the disputed points, SecurityProfiling has backed away from its cited evidence, making no reference to these definitions. *See* Dkt. 91 at 9-10. SecurityProfiling cannot avoid the proper construction of this term by ignoring the relevant evidence, all of which supports Trend Micro's position. Neither of SecurityProfiling's two arguments warrant departing from it.

First, SecurityProfiling argues that an IPS need not process network traffic "packets" because (1) an IPS and a firewall are part of the same thing, (2) a firewall need not process traffic "packets," and (3) therefore an IPS likewise need not process such packets. *See* Dkt. 94 at 11. SecurityProfiling's progression is illogical and inconsistent with the patents' disclosure. As a threshold matter, a firewall and an IPS are two different things and the functionality of one cannot be equated to the other. Indeed, SecurityProfiling cites to nothing in the specification which supports its conflation of a firewall and an IPS and the claims separately recite both firewalls and IPSs (and/or the functionality thereof). *See, e.g.*, '644 Patent, Claim 1; '069 Patent, Claim 2. Consistent with this, Figure 11 depicts both the IPS "Inline Sensor" and the "Perimeter Firewall" separately. *See* '644 Patent, Fig. 11. Moreover, monitoring and processing packets is fundamental to what a firewall does – otherwise it could not determine where network traffic was directed or when to drop or allow network traffic as discussed in the patents. *See, e.g.*, Dkt. 95, Ex. A-5 at 141 (13:14-37) ("***A common function of a firewall 212 is to examine packets*** coming from the wide area network 152 and then either to let them through or block them . . . .") (emphasis added).

Second, SecurityProfiling argues that the claims only require the IPS to "be capable of detecting and preventing vulnerability exploits" and need not do so in real time. *See* Dkt. 94 at 12. However, as explained in Trend Micro's opening brief, preventing an intrusion requires an IPS to take action in real time, as letting malicious network traffic to pass and dealing with it later does not "prevent" an intrusion, it permits it. *See* Dkt. 91 at 9-10. This real time monitoring and processing of network packets by an IPS is expressly called out in the specification and properly reflected in Trend Micro's construction. *See id.*; *see also Phillips v. AWH Corp.*, 415 F.3d 1303, 1316; *GPNE*, 830 F.3d at 1370; *VirnetX, Inc. v. Cisco Sys., Inc.*, 767 F.3d 1308, 1318-19 (Fed. Cir. 2014). Again, SecurityProfiling appears to depart from the unambiguous language of the claims and specification to potentially argue that the term covers fundamentally different anti-virus scanning technology that the patents never purported to invent.

C. <u>"firewall" (Claim Term 3 – see Ex. 1-A at A8)</u>

The parties generally agree on the construction of "firewall" and the evidentiary bases for that construction. The one disagreement concerns SecurityProfiling's proposal to remove the word "all" from an established definition both parties otherwise agree upon. *Compare* Dkt. 94 at 12 (proposed constructions) *with* Dkt. 92, Ex. 1-I at A158-A159 *and* Ex. 1-C at A133. SecurityProfiling's proposed deletion of the word "all" is contrary to the fundamental purpose of a firewall, as confirmed by its consistent use throughout the specification, at the time of the invention. SecurityProfiling cannot avoid this fact by errantly claiming that Trend Micro is trying to import additional elements. *See* Dkt. 94 at 12-13. Neither of SecurityProfiling's two arguments warrants adopting its modified definition.

First, SecurityProfiling attempts to explain, without any support from the record, that "[w]hether any or all information passes through a firewall is a network design decision" and based on the "configuration" of the network or firewall. *See id.* However, by definition, in order

for a firewall (which acts as a gateway or barrier that filters incoming traffic and prevents direct communication with the devices it protects) to perform its basic function, all information directed to the devices it protects must pass through the firewall. As detailed in Trend Micro's opening brief, this is fully consistent with all descriptions and uses of a firewall in the specification (a fact that SecurityProfiling does not address, let alone dispute) and the extrinsic evidence proffered by the parties. *See* Dkt. 91 at 10-11. SecurityProfiling's hypothetical design considerations are untethered to any evidence in the record and SecurityProfiling offers no explanation for how they make any sense in the context of the patents-in-suit and their purported inventions. They do not warrant departing from a construction fully supported by the evidence.

Second, SecurityProfiling again premises its construction on using the word "typically" to excise a swath of a provided glossary definition. *See* Dkt. 94 at 13 & n.4. As a threshold matter, this premise is flawed, as how a term is "typically" understood by a person of ordinary skill in the art is centrally relevant to the proper construction of a term and categorically disregarding and deleting it is plainly improper. Moreover, SecurityProfiling's argument is still misplaced even under its own premise. In addition to ignoring the intrinsic evidence entirely, SecurityProfiling fundamentally misunderstands the language *preceding* the word "typically" in its cited definition. This language explains that "a firewall prevents computers on a network from communicating directly with external computer systems." *See* Dkt. 91 at 10-11; Dkt. 92, Ex. 1-C at A133. The only way to accomplish this is by monitoring "all" traffic entering or leaving the network—otherwise direct communication is not "prevent[ed]." Consistent with this, the glossary definition goes on to explain "all information passing between the networks and external system must travel" through the firewall. *See id.* This is also reinforced by the Microsoft Computer Dictionary that is actually contemporaneous with the invention, which

states: "a firewall prevents computers in the organization's network from communicating directly with computers external to the network and vice versa." *See* Dkt. 91 at 10; Dkt. 92, Ex. 1-I at A158-A159. The dictionary similarly goes on to explain that "all communication is routed" through the firewall's proxy server. *See id.*

D. "remediation technique" (Claim Term 4 – see Ex. 1-A at A8)

SecurityProfiling's open-ended construction of "remediation technique" asks the Court to ignore that "remediation" and "mitigation" are different words with different meanings and disregard the specification's repeated explanations of the fundamental differences between mitigation and remediation techniques. The patent specification discusses both remediation techniques that fix a vulnerability and mitigation techniques that block a present attack that seeks to exploit a vulnerability that has yet to be fixed. *See* 13:10-13 ("It may then have the intelligence to determine if any machine on the network is susceptible to the attack, ***remediate the vulnerability, mitigate the attack***, and verify policy compliance.") (emphasis added).[2] SecurityProfiling's argument conflates these basic concepts that the intrinsic evidence consistently demonstrates are different. Accordingly, Trend Micro's construction should be adopted for at least the following three reasons.

First, SecurityProfiling points to the specification's discussion of using a firewall to mitigate an attack and argues any construction of "remediation technique" must cover such use of a firewall and therefore must include the word "counteract." *See* Dkt. 94 at 10. SecurityProfiling's argument conflates mitigation techniques (such as addressing an attack with a

[2] This difference can be analogized to the real world example of a leaky roof. When it rains, and the roof beings leaking, a person has two options to deal with the problem. First, the person may mitigate the effect of the rainwater (the "attack") passing through the leak (the "vulnerability") by placing a bucket under the leak to keep the water from running onto the floor. This approach would "mitigate" the current "attack" but would not "remediate" the hole in the roof. Second, the person can patch or plug the hole in the roof to remediate or correct the "vulnerability."

firewall) with remediation techniques (such as patches or updates). The specification never refers to the firewall *mitigation* technique quoted by SecurityProfiling as a "remediation technique." Indeed, the passage SecuirtyProfiling quotes is followed by discussion that distinguishes "remediation techniques" (such as applying a patch or update to a vulnerable device) from the cited firewall mitigation technique. *See* '699 Patent, 4:55-67. The description in the specification regarding the IPS's mitigation of an attack similarly highlights this difference and the error in SecurityProfiling's argument for its construction. *See, e.g.*, 19:34-37 ("[I]f the destination IP is vulnerable to the attack, the in-line Sensor is commanded to immediately drop the exploit packets—preventing the attack. ***Further, it remotely remediates the vulnerability" by "deploy[ing] the appropriate update to the machine or device*** . . . .") (emphasis added). Despite its reliance on the patent's discussion of a firewall, SecurityProfiling can point to nothing in the claim language or specification of the '699 Patent suggesting—much less requiring—that a remediation technique be construed to encompass such use of a firewall.[3]

Second, SecurityProfiling's argument that Trend Micro's construction will exclude the "preferred embodiment" for using a firewall is similarly flawed. *See* Dkt. 94 at 14. SecurityProfiling's emphasis on firewall *mitigation* techniques overlooks the specification's separate discussion of a "preferred embodiment" for the *remediation* techniques at issue. *See* '699 Patent, 5:39-42 ("In the preferred embodiment, database 146 includes vulnerability and remediation information such that, for at least one vulnerability, multiple methods of remediating

[3] To the contrary, the specification makes clear that the remediation techniques are applied to one or more vulnerable devices, not to the firewall. *See* '699 Patent, 4:61-67 ("the remediation technique(s) are applied (1) to the machine that was attacked, (2) to all devices subject to the same vulnerability (based on their real-time software patch, policy, and configuration status), or (3) to all devices to which the selected remediation can be applied.");'699 Patent, 5:15-20 ("the remediation can be selectively applied to only those devices subject to the vulnerability").

the vulnerability are specified."). [4] The '699 Patent claim at issue recites remediation techniques and makes no mention of a firewall or mitigation techniques. SecurityProfiling does not and cannot assert that Trend Micro's construction does not encompass the preferred embodiment of what is claimed. This is consistent with Federal Circuit authority that a single claim need not encompass all subject matter and every last feature described in a specification, and the fact that SecurityProfiling did not draft this claim to do so here. *See AllVoice Computing PLC v. Nuance Communications, Inc.*, 504 F.3d 1236, 1248 (Fed. Cir. 2007) ("[E]ach claim need not include every feature of an invention. . . . Thus every claim need not contain every feature taught in the specification."). When SecurityProfiling desired to draft a claim that included firewall-based mitigation techniques or other features, it knew how and did so expressly in numerous other related patents, including the '644, '069¸'431, '686, and '708 Patents asserted here. The '699 Patent includes no such claim language and SecurityProfiling's efforts to shoehorn it into an improperly broad construction of "remediation technique" is in error.[5]

Third, as discussed in Trend Micro's opening brief, SecurityProfiling appends an open-ended list of purportedly exemplary remediation techniques. This unbounded list of "examples"

[4] The specification also refers to multiple "preferred embodiments." *See* '699 Patent, 2:47 ("In this preferred embodiment . . ."); 5:30 ("In a preferred embodiment . . ."); 5:39 ("In the preferred embodiment . . ."). This includes the "preferred embodiment" in the specification cited by SecurityProfiling ('699 Patent, 5:26-29) which merely states that it is preferred for the security database to be detached from any particular application on the network and has nothing to do with claimed "remediation techniques." *See* '699 Patent, 5:26-29 (explaining that "[i]n some embodiments, the database 146 is integrated into another device, such as firewall 131 or router 133, or an individual device on the network" but that "the network-attached device embodiment described above in relation to Figures 1-4 is preferred").

[5] *See August Technology Corp. v. Camtek, Ltd.*, 655 F.3d 1278, 1285 (Fed. Cir. 2011) ("The mere fact that there is an alternative embodiment disclosed . . . that is not encompassed by [the] claim construction does not outweigh the language of the claim, especially when the court's construction is supported by the intrinsic evidence."); *see also id.* ("This is especially true where, as here, other unasserted claims in the parent patent cover the excluded embodiments.") (internal citations and quotations omitted).

will be unhelpful to the jury and is unsupported by the specification; contrary to SecurityProfiling's suggestion, the proffered examples go beyond "the exact words the inventors used to define the scope of the term." *Compare* Dkt. 94 at 13-14 (SecurityProfiling's construction) with '699 Patent, 5:1-5.

E. "patch, policy setting, and configuration option" terms (Claim Terms 5 and 6 – see Ex. 1-A at A9)

SecurityProfiling's arguments regarding the "patch, policy setting, and configuration option" terms miss the point at issue and contradict Federal Circuit authority.

1. The '708 and '431 Patents must include each mitigation type

For Claim Term 5, SecurityProfiling's arguments attack a grammatical straw man. The database described in the specification and recited by the claims requires a collection of techniques where each technique has a particular type. Consistent with this, Trend Micro's construction requires that this collection of techniques include at least one technique of each recited type recited in the claim term. *See* Dkt. 91 at 15-16. Rather than address this construction, SecurityProfiling argues against a single technique simultaneously being every recited type—*i.e.*, a "patch," a "policy setting," and a "configuration option." *See* Dkt. 94 at 15-16. This is neither logical nor Trend Micro's construction. As explained in Trend Micro's opening brief, both the case law interpreting similar terms and the intrinsic record support Trend Micro's actual proposal above. *See id.*[6]

SecurityProfiling's citation to the abstract is similarly unavailing, as it recites language more similar to a Markush Group, which, as explained in Trend Micro's opening brief, is

[6] In a further attack on its straw man, SecurityProfiling points to a dependent claim that depends from a different independent claim that is not at issue and recites that each of the types are required for different techniques. *See* Dkt. 94 at 15-16. This adds nothing to warrant departing from the clear meaning of the claim language as reflected in Trend Micro's construction.

different than what is recited here. *See* Dkt. 91 at 15. Moreover, the abstract was written during prosecution of a continuation patent nearly a decade after SecurityProfiling's original application was filed. Accordingly, it is of little moment to a skilled artisan's understanding of the claim language at the time of the alleged invention, as it did not exist at that time.

2. The '708 and '431 Patents are indefinite as it is unclear how patch, policy setting, and configuration option types can also be firewall or IPS techniques

The claim terms for the '431 and '708 Patents (*i.e.*, Term 5) are also indefinite. Trend Micro is not arguing enablement, but rather that the terms are indefinite because they fail to "inform those skilled in the art about the scope of the invention with reasonable certainty." *See Nautilius, Inc. v. Biosig Instruments, Inc.*, 134 S. Ct. 2120, 2129 (2014). As Trend Micro's opening brief explained, there is nothing in the specification suggesting—let alone explaining how—a mitigation technique can be both a firewall or IPS technique and also one of the required types. *See* Dkt. 91 at 16. SecurityProfiling's response only highlights this problem.

SecurityProfiling claims, without support, that "a firewall, for example, could use a mitigation technique such as dropping or rejecting a connection request, and that such a technique would classified as a policy setting (i.e., the policy of the firewall and/or IPS) or configuration option (i.e., how the firewall and/or IPS are configured to respond)." *See* Dkt. 94 at 17. Even accepting this unadorned attorney argument, SecurityProfiling itself cannot delineate meaningful bounds for this claim language. According to this explanation, the same firewall mitigation technique somehow may be both a firewall "policy setting" and a "configuration option" of "the firewall and/or IPS." The law requires more than leaving the public—and, here,even the patentee—guessing as to what falls within or outside of the scope of a claim's language. Nor does the specification provide assistance, as SecurityProfiling cites only to a discussion of a security server informing a firewall whether or not to allow a pending external

connection request to proceed.[7] *See id.* The specification says nothing regarding modifying policies or configurations for firewalls or IPSs.[8] Moreover, the discussion of the patch, policy setting, and configuration options in the specification is in the context of remediating a vulnerability on a device and is unconnected to a firewall or IPS. *See, e.g.*, supra, Section III.D. Thus, the claim terms fail to inform with reasonable certainty those skilled in the art about the scope of the invention and are therefore indefinite.

3. The '699 Patent includes a "closed" Markush Group

For the '699 Patent (Claim Term 6), SecurityProfiling repeats practically identical arguments as for Claim Term 5 despite their different language. As discussed in Trend Micro's opening brief, Trend Micro agrees that the '699 Patent recites a Markush Group which, unlike the '431 and '708 Patents, does not require all three types to be present. *See* Dkt. 91 at 14. However, as customary for a Markush Group, the group is closed and does not allow any other types to be present. *See id.* SecurityProfiling makes no effort to rebut the case law presented by Trend Micro or argue that the intrinsic record requires other types to be allowed. Thus, for the reasons explained in its opening brief, Trend Micro's construction should be adopted.

F. <u>"occurrence," "occurrence packet," and "attack" (Claim Terms 7-9 – see Ex. 1-A at A9)</u>

As with many of the other claim terms discussed herein, SecurityProfiling again mischaracterizes the specification in an apparent effort to overly broaden the claims' scope to

[7] SecurityProfiling erroneously cites to a passage from the specification discussing how the "Security server 135 sends result signal 217 back to firewall 131 with an indication of whether the connection request should be granted or rejected." *See* '708 Patent, 4:13-21; *see also* '644 Patent, 4:13-21 for an identical passage. However, this does not support SecurityProfiling's argument that firewalls have "policy settings" and "configuration options" pursuant to the purported invention.

[8] The parties' agreed constructions for "patch," "policy setting," and "configuration option" bear no relation to or indication of firewalls or IPSs but, rather, refer to modifying policies and configurations on devices.

sweep in security applications it did not invent. *See* Dkt. 94 at 19. In contrast, Trend Micro's construction ties the claims, and their recitation of occurrences and attacks, to the specification and the purported invention claimed.[9] *See* Dkt. 91 at 16-17. The claims (and the specification) are directed to identifying and preventing "occurrences" and "attacks" through use of firewall and IPS mitigation techniques, which, as discussed herein, the parties agree involve protecting devices from certain network traffic. *See, e.g.*, Supra, Sections III.B, III.C and corresponding constructions for IPS and firewall, respectively. SecurityProfiling's arguments fail to support its own construction and reinforce why Trend Micro's should be adopted for four reasons.

First, Trend Micro's construction does not limit "occurrence" to a single occurrence packet. Rather, it makes clear that an occurrence packet is a single packet within an occurrence, which the claim language makes clear must consist of one or more packets. *See* Dkt. 91 at 17; *see also* '069 Patent, Claim 2 ("occurrence includ[es] at least one . . . occurrence packet directed to the at least one networked device"). SecurityProfiling's construction ignores this aspect of an "occurrence" and has no response to the claim language fact explicitly reciting that an occurrence consists of "packets."

Second, SecurityProfiling refers to a brief reference in the specification regarding how "blended attacks may now utilize metamorphic or polymorphic abilities to change their signatures to avoid detection." *See* Dkt. 94 at 19 (quoting '644 Patent, 8:11-13). SecurityProfiling continues with unsupported attorney argument as to why one of skill in the art would know that "occurrences" undetected in network traffic may still target computer networks at a later time. *See id.* This passage from the specification does not support SecurityProfiling's

[9] As discussed in Trend Micro's opening brief, Trend Micro agrees that "occurrence" and "attack" should be construed similarly, but the usage of "occurrence," an inherently ambiguous term, requires construction (which SecurityProfiling does not dispute).

construction, as it is directed to the state of the prior art and a reason for why "organizations are now deploying a multi-tiered network defense strategy" to combat such attacks (*e.g.*, such as those that deploy both firewalls and IPSs, which were readily known in the art). *See* '644 Patent, 8:11-19. It says nothing as to SecurityProfiling's purported invention. If it did, SecurityProfiling would not need to resort to an overbroad definition from a non-technical dictionary that is divorced from the specification.[10] As discussed, the purpose of the purported invention is directed to identifying and preventing attacks and occurrences through firewall and IPS mitigation techniques. Allowing SecurityProfiling to stretch the construction of "occurrence" to scenarios that are unaddressed and unsupported in the specification and otherwise have no bearing on the claims is contrary to a fundamental purpose of claim construction. *See Phillips*, 415 F.3d at 1316 (claims construed based on "what the inventors actually invented"); *see also GPNE*, 830 F.3d at 1370; *VirnetX*, 767 F.3d at 1318.

Third, SecurityProfiling references the same passage in the specification as above that refers to "viruses, worms, and denial of service attacks" and "new blended attacks" to argue that the attacks detected and prevented by a firewall or IPS do not need to include packets. See Dkt. 94 at 20. Again, this passage is referring to the prior art generally and not to attacks identified and prevented by the purported invention. Rather, the claims and specification of the patents-in-suit are directed to preventing attacks in network traffic by firewalls and IPSs, which indisputably take the form of network traffic packets. *See* 4:18-21 ("firewall 133 drops or rejects the connection request 211 as is understood in the art"); 20:4-9 ("[A]n IPS in-line sensor

[10] As discussed in Trend Micro's opening brief, other than its overbroad dictionary definition, SecurityProfiling's extrinsic evidence from "thefreedictionary.com" supports Trend Micro's construction, as it explains that computer network attacks (as opposed to any generic attack) relies upon packets within network traffic. *See* Dkt. 92, Ex. 1-N at A191 ("[Computer network attack] relies on the data stream to execute the attack").

monitors and processes network traffic" and "the in-line Sensor is commanded in real-time to drop the malicious packets."); *see also GPNE*, 830 F.3d at 1370; *VirnetX*, 767 F.3d at 1318.

Fourth, SecurityProfiling's construction introduces the term "computer network" that does not exist in the claims or in the specification's references to occurrences or attacks. In contrast, Trend Micro's construction is consistent with the claim language and the repeated and consistent use throughout the specification, that make clear "attacks" and "occurrences" target one or more devices, not an undefined computer network. *See* Dkt. 91 at 17.

Thus, SecurityProfiling's construction which solely relies on overbroad dictionary definitions without reference to the claims or specification should be rejected.

IV. CLAIM TERMS GOVERNED BY 35 U.S.C. § 112, ¶ 6

A. The "code" and other "nonce" terms are governed by § 112, ¶ 6

It is well-settled that the Federal Circuit's *en banc* decision in Williamson was a landmark holding that significantly altered the landscape of § 112, ¶ 6 jurisprudence. In doing so, the Federal Circuit sought to deter the "proliferation of functional claiming untethered to § 112, para. 6 and free of the strictures set forth in the statute." *Williamson*, 792 F.3d at 1349. To do so, *Williamson* substantially reduced the presumption against applying § 112, ¶ 6 to terms that do not expressly utilize "means," overruling previous cases such as *Lightning World* that held a strong presumption applied. *See id.* As the Federal Circuit explained, a "nonce" term "can operate as a substitute for 'means' in the context of § 112, para. 6" where it provides only "a generic description for software or hardware that performs a specified function." *Williamson*, 792 F.3d at 1349-50. Such is the case here, as five of the six patents and all but one asserted claim merely recite software elements in purely functional terms.

In opposing the application of § 112, ¶ 6, SecurityProfiling relies almost exclusively on cases decided before *Williamson* and advances arguments that are contrary to its holding and that

have been rejected by a number of courts thereafter. *See* Dkt. 94 at 23-25. Accordingly, § 112, ¶ 6 should apply to the functionally claimed limitations here.

1. The "code" and other "nonce" terms fail to connote sufficiently definitely structure and therefore should be governed by § 112, ¶ 6

SecurityProfiling argues that the use of "code" in the claims inherently connotes structure by itself, unlike the term "module" in *Williamson*, and precludes the application of § 112, ¶ 6. Dkt. 94 at 23-25. Beyond the practical effect of creating an irrebuttable presumption never before recognized by any court, the argument cannot be squared with *Williamson* or cases applying it. As *Williamson* explained, a claim term need not use the word "means" to fall within § 112, ¶ 6 if it merely provides "a generic description for software or hardware that performs a specified function." *See Williamson*, 792 F.3d at 1350 (internal quotations and citations omitted).[11] It is beyond legitimate dispute that the recitation of "code for" in the claims here is just such a "generic description for software." *Id.* Indeed, the claims here include terms (*i.e.*, references to "code" without more) that are more generic than the software/hardware elements at issue in *Williamson*, which held that the phrase "distributed learning control module" was an insufficiently particular "nonce" term that required the application of § 112, ¶ 6. *See id.* at 1351–52. *See also* Dkt. 94 at 23-25.[12]

[11] Contrary to SecurityProfiling's misplaced accusations (Dkt. 94 at 23), Trend Micro never claimed that *Williamson* expressly found "code" to require application of § 112, ¶ 6.

[12] The fact that some claims here also recite a "computer readable medium" does not save the limitations from application of § 112, ¶ 6. *See Global Equity Management*, 2016 WL 7416132, at *29-30 (applying § 112, ¶ 6 to claim reciting "A computer program product for use on a computer system with a memory, a display and multiple operating system, the computer program product comprising a computer usable medium . . ."). In addition, not all of the asserted independent claims recite "computer-readable medium" in the preamble. *See, e.g.*, '431 Patent, Claim 15; '708 Patent, Claim 18; '686 Patent, Claim 1. Moreover, the claims at issue here recite a "computer program product," (*e.g.*, a product claim) which also comprises multiple "code" modules (similar to in *Global Equity Management*). The recited "code" here is not the claim as a whole as defined in the preamble but comprises distinct modules or components of code within

Consistent with this, other courts applying *Williamson* have held that terms similar to, and even more descriptive than, the "code for" terms here were governed by § 112, ¶ 6. *See, e.g.*, *Zeroclick LLC v. Apple Inc.*, No. 15-cv-04417-JST, 2016 WL 5477115 at *4–*6 (N.D. Cal. August 16, 2016) (holding that the claim terms "program that can operate …" and "user interface code" did not "recite any structure whatsoever, let alone 'sufficiently definite structure.'" citing *Williamson*, 792 F.3d at 1349; *id.* at 1351–52); *Verint Sys. Inc. v. Red Box Recorders Ltd.*, 166 F. Supp. 3d 364, 379-80 (S.D.N.Y. 2016) (holding that even considering the proffered dictionary definition of "application" as "[a] collection of software components used to perform specific types of user-oriented work on a computer," the term "fails to provide sufficient additional structure"); *Global Equity Management (SA) Pty. Ltd. v. Expedia, Inc.*, No. 16-cv-95-RWS-RSP, 2016 WL 7416132, at *29-30 (E.D. Tex. Dec. 22, 2016) ("the program code is defined only by the function that it performs").[13] Similarly, courts have also found that "code means" does not rebut the presumption of § 112, ¶ 6, because "'Code,' like 'commands,' connotes software, and does not disclose 'a specific physical structure that performs the function.'" *See, e.g.*, *Tobii Tech. AB v. Eye Tribe APS*, No. 13-cv-05877, 2016 U.S. Dist. LEXIS 7841, *18-19 (N.D. Cal. Jan. 22, 2016) (*quoting Altiris, Inc. v. Symantec Corp.*, 318 F.3d 1363, 1376 (Fed. Cir. 2003)).

---

the claim. *Compare* '644 Patent, Claim 1 *with Syncpoint Imaging, LLC v. Nintendo of Am. Inc.*, No. 2:15-cv-00247, 2016 WL 55118, at *23 (E.D. Tex. Jan. 5, 2016) (declining to apply § 112, ¶ 6 to "instructions" defined in the claim's preamble: "A computer readable storage medium having stored data representing instructions executable by a computer to generate commands to control a cursor.").

[13] SecurityProfiling attempts to distinguish Trend Micro's cited cases by claiming that, unlike the claims at issue in those cases, "the disputed terms in this case rest on a much more definite structural foundation" or that "the word 'code' is lent structural significance by a substantial number of additional claim terms which are understood by an ordinarily skilled artisan as being names for structure." *See* Dkt. 94 at 26-28. However, as discussed further below, much like the cases cited by Trend Micro, the additional language recited in the *functions* here similarly do not describe structure for performing those functions. *See* Section IV.A.2, *infra*.

Indeed, adopting SecurityProfiling's argument would result in the sort of pure functional claiming that the Federal Circuit, in *Williamson* and other cases, has repeatedly cautioned is improper and explained that § 112, ¶ 6 exists to prevent:

> The point of the requirement that the patentee disclose particular structure in the specification and that the scope of the patent claims be limited to that structure and its equivalents is to avoid pure functional claiming. . As this court explained in *Medical Instrumentation & Diagnostics Corp. v. Elekta AB*, 344 F.3d 1205, 1211 (Fed. Cir. 2003), "if the specification is not clear as to the structure that the patentee intends to correspond to the claimed function, then the patentee has not paid the price but is attempting to claim in functional terms unbounded by any reference to structure in the specification."

Aristocrat Techs. Australia Pty Ltd. v. Int'l Game Tech., 521 F.3d 1328, 1333 (Fed. Cir. 2008); *see also Williamson*, 792 F.3d at 1349-50 (noting "proliferation of functional claiming untethered to § 112, para. 6 and free of the strictures set forth in the statute" is inconsistent with Congressional intent); *EON Corp. IP Holdings LLC v. AT&T Mobility LLC*, 785 F.3d 616, 623 (Fed. Cir. 2015) (reference to generic computing items "as corresponding structure for a software function does nothing to limit the scope of the claim and avoid pure functional claiming.") (internal citation and quotation omitted); *Biomedino, LLC v. Waters Techs. Corp.*, 490 F.3d 946, 948 (Fed. Cir. 2007) ("in return for generic claiming ability, the applicant must indicate in the specification what structure constitutes the means").[14]

The claims here fall squarely within this Federal Circuit guidance. As noted in Trend Micro's opening brief, the "code" terms here are written in the same format as a traditional means-plus-function limitation, merely replacing the words "means for" with "code for" or "code that" and reciting a function performed by the "code." Dkt. 91 at 19-21. As with

[14] *Cf. Augme Technologies, Inc. v. Yahoo!, Inc.*, 755 F.3d 1326, 1338 (Fed. Cir. 2014) (holding "[c]ode assembler instructions" was insufficient structure to render a means-plus-function claim term definite); *Altiris*, 318 F.3d at 1376 (Fed. Cir. 2003) (holding "commands," in the form of computer software, within a claim limitation did not constitute sufficient structure to rebut presumption of means-plus-function treatment).

"module" in *Williamson*, the term "code" merely acts as a "generic description for software," denotes no more structure than the word "means," and simply serves as a black box to perform the specified function. *Williamson*, 792 F.3d at 1350. The number and variety of claimed functions performed by "code" reinforces that the term is nothing more than a generic placeholder and is simply a nonce word in place of "means." The "code" terms do not otherwise provide any structural significance to the "computer program product" or "system" claims of the patents-in-suit. Thus, "code" and the other "nonce" terms should be governed under § 112, ¶ 6.[15]

2. SecurityProfiling's emphasis on terms defining the *functions* to be performed does not provide structure that performs those functions

SecurityProfiling points to various words recited in the functions to be performed by the claimed code that it contends were "understood by persons of ordinary skill in the art to have a sufficiently definite meaning as the name for structure" to argue that § 112, ¶ 6 should not apply. *See, e.g.*, Dkt. 94 at 29 (quoting *Williamson*, 792 F.3d at 1349).[16] The argument misses the point and has been rejected by the Federal Circuit.

The relevant inquiry is not whether a function to be performed makes reference to some structure, but rather whether the claim recites sufficiently definite structure to *perform* the recited function. As the Federal Circuit explained in *Williamson*, "§ 112, para. 6 will apply if the

[15] SecurityProfiling does not meaningfully dispute that the "processor," "data storage," and "component" nonce terms fail to impart sufficiently definite structure. Rather, it primarily argues that additional language within the functional parts of the claim limitations impart sufficient structure. *See, e.g.*, Dkt. 94 at 31-32. However, as discussed below, the additional language cited by SecurityProfiling does not sufficiently connote structure as to avoid application of § 112, ¶ 6. *See* Section IV.A.2, *infra*.

[16] SecurityProfiling's approach also appears to rely heavily on *Lightning World, Inc. v. Birchwood Lighting, Inc.*, 382 F.3d 1354, 1359-60 (Fed. Cir. 2004), which was explicitly overruled by *Williamson*. See Dkt. 94 at 23 ("A claim term does not fall under § 112(f) if it 'is used in common parlance or by persons of skill in the pertinent art to designate structure, even if the term covers a broad class of structures and even if the term identifies the structures by their function.'"). *Lightning World* followed the strong presumption against application of § 112, ¶ 6, which was abrogated by *Williamson*. *See Williamson*, 792 F.3d at 1349.

challenger demonstrates that ***the claim term fails to recite sufficiently definite structure . . . for performing that function***." 792 F.3d at 1348 (internal citations and quotations omitted) (emphasis added); *see also Kemco Sales, Inc. v. Control Papers Co., Inc.*, 208 F.3d 1352, 1361 (Fed. Cir. 2000) (§ 112, ¶ 6 may apply "if the claim limitation is determined not to recite sufficiently definite structure ***to perform the claimed function***") (emphasis added).[17]

When this controlling question is considered, SecurityProfiling's argument fails for three primary reasons: (1) SecurityProfiling's purported structural terms do not perform the claimed functions, they merely appear in the description of the functions themselves; (2) a well-known or conventional component does not necessarily connote structure itself and/or does not necessarily impart structure onto an otherwise functionally claimed term; and (3) SecurityProfiling's approach has been rejected by the Federal Circuit in the context of "brick-and-mortar" patents involving far more concrete structure than the claims include here.

First, SecurityProfiling does not meaningfully contend or explain how any of the words it selected from the recited functions constitute structure that performs those functions as the law requires.[18] Nor can it. As illustrated in the examples below, the only thing recited in the claims for performing those functions is "code for" doing so or equivalent "nonce" language. The Federal Circuit rejected a similar argument in *Laitram Corp. v. Rexnord, Inc.*, 939 F.2d 1533, 1536 (Fed. Cir. 1991). In *Laitram*, the Federal Circuit noted that the "recited structure tells only what the means-for-joining does, not what it is structurally" and that "the structural description

[17] In assessing the relevant question, a minimal semblance of structural support that does not otherwise describe the sufficiently definite structure for performing the function is insufficient to avoid the application § 112, ¶ 6. *See Williamson*, 792 F.3d at 1349 ("We also overrule the strict requirement of a showing that the limitation essentially is devoid of anything that can be construed as structure." (internal citations and quotations omitted)).

[18] SecurityProfiling's exercise of isolating items from the recited functions for consideration breaks from its emphasis elsewhere on the need to consider a claim limitation as a whole. *See* Dkt. 94 at 23.

in the joining means clause merely serves to further specify the function of that means." *Id.* Here, each of the terms that purportedly indicate structure are extraneous to the claimed code:

- **Claim Terms Concerning Multiple Mitigation Techniques (Claim Terms 10-23):** According to SecurityProfiling, the additional terms "firewall," "IPS," and "user input" provide sufficiently definite structure to, for example, Claim 1 of the '644 Patent. *See* Dkt. 94 at 28-31. However, SecurityProfiling does not contend that any of these items (well-known or not) actually perform the recited functions—nor can they. For example, the function "providing a user with one or more options to selectively utilize different occurrence mitigation actions of diverse occurrence mitigation types . . ." is performed by the claimed code, not an IPS or Firewall.[19] Similarly, "user input" does not provide any additional sufficiently definite structure because "user input" also does not "provide a user with . . . options." *See also, e.g.*, *Zeroclick*, 2016 WL 5477115 at *4–*6 (construing "user interface code" as § 112, ¶ 6 where "user interface" did not provide sufficient structure). Rather, the claimed code here is only defined by the function (*i.e.*, the "providing") it performs. *See Global Equity Management*, 2016 WL 7416132, at *29-30 ("the program code is defined only by the function that it performs").
- **Claim Terms Concerning Identifying an Occurrence in Connection with a Device (Claim Terms 30-31):** Similarly, for Claim 1 of the '644 Patent,

[19] Moreover, the claim limitations here typically utilize open-ended language which merely "includes," for example, firewalls and IPSs. Accordingly, these purported well-known terms do not meaningful limit or define the structure of the "code" or function thereof. *See Altiris*, 318 F.3d at 1376 ("The claim language uses 'including'—an open term—which suggests that the two sets of 'commands' are not sufficient structure; rather, something else is needed.").

SecurityProfiling claims that the recitation of "occurrence" and "plurality of devices" imparts sufficiently definite structure to the claim limitations that recite, for example, "identifying an occurrence in connection with at least one of the plurality of devices." *See* Dkt. 94 at 34-35. But again, SecurityProfiling does not contend that the occurrence or devices actually perform the recited function. That "occurrences" (or "attacks") and "devices" are well-known does not impart sufficiently definite structure for performing the function that requires ***identifying*** an occurrence. Again, the claimed code is only defined by the function (*i.e.*, the "identifying") it performs. *See Global Equity Management*, 2016 WL 7416132, at *29-30.

- **Claim Terms for Determining Whether Devices Are Actually Vulnerable to an Occurrence or Attack (Claim Terms 32-35):** Finally, and similar to the above, SecurityProfiling argues that the recitation of "vulnerability," "plurality of devices," and "occurrence/attack" imparts sufficiently definitely structure to the claim terms for determining whether devices are actually vulnerable to an occurrence or attack. *See* Dkt. 94 at 35-36. However, like the above, SecurityProfiling does not contend that the limitations require that the recited "occurrences/attacks" and "devices" perform any portion of the recited function, nor do they. The recited functions require a ***determination*** regarding "occurrences/attacks" and "devices" and these terms do not impart structure for performing the recited function. In addition, the inclusion of "vulnerability information" with respect to the recited determination merely further specifies the recited function and is insufficient to perform the function itself. The claim

> limitations do not otherwise create vulnerabilities or define vulnerabilities on a computer system—the claimed code thus is only defined by the function it performs. *See Global Equity Management*, 2016 WL 7416132, at *29-30.

The remaining terms that SecurityProfiling claims provide sufficiently definite structure, including "software update," "network," "data storage," "operating system," "patch," "policy," and "configuration," are no different. As with the above, they merely further specify the recited functions rather than impart sufficiently definite structure that performs those functions.

Second, SecurityProfiling identifies various instances where certain terms in each function are either disclosed in (1) the specification of the patents-in-suit or (2) contemporaneous patents published or issued around the time the first application of the patents-in-suit was filed. *See, e.g.*, Dkt. 94 at 29 ("An intrusion prevention system is disclosed in the specification" and "Plaintiff points to patents issuing contemporaneously with the priority date of the Patents-in-Suit"). However, this exercise misses the point. Merely because an item from the function of the § 112, ¶ 6 term was known at the time of the invention does not provide any support that the item itself connotes structure to avoid application of § 112, ¶ 6 to functionally-claimed limitations. Indeed, there is no connection that a conventional and well-known term contemplated by a function is necessarily understood to have "sufficiently definite meaning as the name for structure." Moreover, it certainly does not follow that the item imparts any structure to the claimed "code" when the item itself does not perform the recited function (as discussed above).

Similarly, the patents-in-suit do not purport to invent a new or novel firewall or IPS, which SecurityProfiling readily admits in its brief and in the specification of the patents-in-suit. *See, e.g.*, Dkt. 94 at 29 ("[A]n intrusion prevention system is a term an ordinarily skilled artisan

would have understood at the date to which the Patents-in-Suit claim priority."); *id.* at 29-30 ("[F]irewall is a term an ordinarily skilled artisan would have understood at the date to which the Patents-in-Suit claim priority."); '644 Patent, 4:19-21 ("firewall 133 drops or rejects the connection request 211 as is understood in the art"). Rather, as discussed above, the purported invention merely implicates the conventional and well-known security systems and does not claim the firewall or IPS themselves. At best, the claims purport to provide options for potentially utilizing a conventional firewall or IPS. Accordingly, claiming that firewalls and IPSs, amongst other terms, are well-known and conventional does nothing to impart structure on the functionally-claimed limitations (especially where they do not actually perform the function).

Third, as discussed above, the relevant structure to avoid application of § 112, ¶ 6 must be sufficiently definite "for performing that function." *See Williamson*, 792 F.3d at 1349; *Kemco Sales*, 208 F.3d at 1361. Indeed, SecurityProfiling's approach would foreclose § 112, ¶ 6 from more traditional mechanical or "brick-and-mortar" patents that include structural characteristics but fail to provide structure for performing the entire function.[20] For example, in *Laitram Corp. v. Rexnord, Inc.*, the patentee attempted to avoid application of § 112, ¶ 6 for "means for joining said pluralities [of link ends] to one another so that the axes of [certain holes are arranged in a particular configuration]." 939 F.2d at 1535-36. The Federal Circuit held that, like here, the "recited structure tells only what the means-for-joining does, not what it is structurally." *See id.* ("The recitation of some structure in a means plus function element does not preclude the applicability of section 112(6). For example, in this case, the structural description in the joining means clause merely serves to further specify the function of that means."). This is identical to

[20] While the presumption of § 112, ¶ 6 flips depending on whether "means" is expressly recited or not, the general test for assessing the applicability of § 112, ¶ 6 remains the same: whether or not the "claim limitation itself recites sufficiently definite structure to perform the claimed function." *See Kemco Sales*, 208 F.3d at 1361.

the case here, where, for example, the recited firewalls and IPSs merely identify the types of mitigation actions the purported invention provides to the user without providing sufficiently definite structure for performing, for example, the function of providing options to a user. *See Cross Medical Products, Inc. v. Medtronic Sofamor Danek, Inc.*, 424 F.3d 1293, 1308 (Fed. Cir. 2005) (in a claim directed to a spinal implant, the claim phrase "securing means" was a means-plus-function limitation "[b]ecause there is insufficient structure recited for performing the specified function" since the threads alone did not perform the securing function and additional structure was required); *Unidynamics Corp. v. Automatic Products Intern., Ltd.*, 157 F.3d 1311, 1320–22 (Fed. Cir. 1998) (*abrogated on other grounds by Egyptian Goddess, Inc. v. Swisa, Inc.*, 543 F.3d 665 (Fed. Cir. 2008)) ("spring means tending to keep the door closed" interpreted to be a means-plus-function limitation even though "spring" was an element of structure in view of the specification's statement that "spring 46 is an example of spring means tending to keep the door closed").

Thus, the claim terms are governed by § 112, ¶ 6 because the claims limitations do not provide sufficient structure to perform the claimed function.

B. The "code" and other nonce terms are indefinite because the specification fails to disclose clearly linked structure to perform each claimed function

SecurityProfiling does not argue, nor can it, that there are sufficient algorithms disclosed in the specification to make the "code" and related terms definite if § 112, ¶ 6 applies. Rather, SecurityProfiling chiefly repeats its flawed arguments addressed above that § 112, ¶ 6 should not apply at all. To be clear, it is no surprise that where courts have found claim terms to *not* fall under § 112, ¶ 6 that those same courts have not applied the requirements of § 112, ¶ 6. SecurityProfiling's citation to a string of such cases is a red herring. *See* Dkt. 94 at 41-42.

SecurityProfiling's three fallback arguments against indefiniteness fare no better. Indeed, all are directly contrary to controlling Federal Circuit precedent.

First, SecurityProfiling suggests that the Federal Circuit's "algorithm rule" (requiring an algorithm be clearly linked as corresponding structure for computer implemented means-plus-function elements, *See Harris Corp. v. Ericsson Inc.*, 417 F.3d 1241, 1253 (Fed. Cir. 2005)) only applies to means-plus-function elements "written in express 'means for'" format. *See* Dkt. 94 at 42. There is no such "magic word" requirement under settled law. If § 112, ¶ 6 applies, its requirements must be met whether a claim term uses "means" or some other nonce term.

Indeed, SecurityProfiling's suggestion is dispelled by the *Williamson* decision itself, which: (1) found § 112, ¶ 6 applied to the claimed "module" term, which did not recite the word "means," (2) held that an algorithm was necessary corresponding structure for the module term ("We require that the specification disclose an algorithm for performing the claimed function."); and (3) found the module term indefinite because the patent failed to disclose a corresponding algorithm clearly linked to the function. *See Williamson*, 792 F.3d at 1351-54.

Second, SecurityProfiling argues that an algorithm is not required even if § 112, ¶ 6 applies because "an ordinarily skilled artisan would understand that the disclosure of the patent encompasses software for the claimed functions and would be able to implement such a program." *See* Dkt. 94 at 43. The Federal Circuit has observed such arguments are meritless. In *EON Corp.* the patentee likewise argued no algorithm was required because "a person of ordinary skill in the art could implement the software function." 785 F.3d at 623. In no uncertain terms, the Federal Circuit explained: "***This argument is meritless***. In fact, ***we have repeatedly and unequivocally rejected this argument***: a person of ordinary skill in the art plays ***no role whatsoever*** in determining whether an algorithm must be disclosed as structure for a

functional claim element." *Id.* (emphasis added). The *EON* court likewise explained that, as SecurityProfiling does here, "[t]he parties also agree that the functions claimed in the terms at issue are all performed by computer software" and "It is ***well-established*** that the corresponding structure for a function performed by a software algorithm is the algorithm itself." *Id.* at 621 (emphasis added).

Third, SecurityProfiling argues that its § 112, ¶ 6 elements do not require an algorithm because the specification purportedly discloses computing "elements well understood by an ordinarily skilled artisan to represent structure." *See* Dkt. 94 at 43. Again, this argument has been squarely rejected. In *EON*, the Federal Circuit made clear that—outside of a narrow *Katz* exception that SecurityProfiling does not argue applies here—"***All other computer-implemented functions require disclosure of an algorithm.***" 785 F.3d at 623 (emphasis added).[21] Here, there is no dispute that the "code for" and similar nonce terms are computer implemented and therefore disclosure of an algorithm is required. *See id.* at 623 (where a § 112, ¶ 6 element "recite[s] a software function, [the patentee] accedes to the reciprocal obligation of disclosing a sufficient algorithm as corresponding structure"). While SecurityProfiling contends its patents disclose "structure" for performing these functions, it does not contend any such structure constitutes an algorithm. In fact, SecurityProfiling merely cites back to general references to firewalls, IPSs, and data storages that are represented merely as boxes in figures, the insufficiency of which Trend Micro has addressed in detail above and in its opening brief.

* * *

[21] The Federal Circuit has held that the *Katz* exception is "narrow" and only applies in "rare circumstances" where a processor can perform a function without any additional "special programming." *See EON*, 785 F.3d at 621-22. SecurityProfiling does not argue the exception applies, nor could it, as it asserts that the claimed functions require "software" programmed to perform the functions.

SecurityProfiling's brief leaves little in dispute concerning the § 112, ¶ 6 issues that are dispositive as to five of the six patents in suit and all but one asserted claim. Defendants respectfully submit that any dispute that is left is readily resolved by controlling Federal Circuit authority. In summary:

- Unless the nonce term "code for" (and related terms)—which is less specific than the "distributed learning control module" addressed in *Williamson*—connotes sufficiently definite structure for performing the varied claimed functions, § 112, ¶ 6 applies.
- There is no dispute that all the § 112, ¶ 6 elements are computer-implemented.
- The Federal Circuit has made clear that all such computer-implemented § 112, ¶ 6 elements require disclosure of an algorithm as corresponding structure.
- There is no dispute that the patents-in-suit do not disclose such algorithms as corresponding structure.

While these § 112, ¶ 6 elements are numerous, briefing here has confirmed that they are resolved by a narrow set of common issues outlined above. Trend Micro respectfully submits that the law is clear and these claims are invalid as indefinite.

Dated: February 12, 2018

Respectfully submitted,

By: */s/ Yar R. Chaikovsky*

Yar R. Chaikovsky, CA Bar No. 175421
yarchaikovsky@paulhastings.com
Michael C. Hendershot, CA Bar No. 211830
michaelhendershot@paulhastings.com
Evan M. McLean, CA Bar No. 280660
evanmclean@paulhastings.com
PAUL HASTINGS LLP
1117 S. California Ave.
Palo Alto, California 94304-1106
Telephone: (650) 320-1800
Facsimile: (650) 320-1900

E. Leon Carter, Bar No. 03914300
Scott W. Breedlove, Bar No. 00790361
CARTER SCHOLER, PLLC
8150 N. Central ExpY., Suite 500
Dallas, Texas 75206
Telephone: (214) 550-8188
Facsimile: (214) 550-8185
Email: lcarter@carterscholer.com
Email: sbreedlove@carterscholer.com

Attorneys for Defendants Trend Micro America, Inc. and Trend Micro, Inc.

CERTIFICATE OF SERVICE

The undersigned certifies that the foregoing document was filed electronically in compliance with Local Rule 5.1(d). As such, this document was served on all counsel who are registered users of ECF on this 12th day of February, 2018.

By: */s/ Yar R. Chaikovsky*
Yar R. Chaikovsky